Explanation of position of the Russian Federation on the initiative to establish a global Points of Contact Directory

Introduction

Since the establishment of CERT-community, the interaction between ICT security experts has been carried out on the basis of unwritten "gentlemen's" agreements that are regularly violated. Considering the evolving nature of threats, both public and private actors have been engaged in search for ways of developing cooperation in this field to maintain peace and security. Hence, a number of organizations that unite national CERTs appeared, for instance, FIRST.

Another solution resulted in the elaboration of non-binding confidence-building measures (CBMs). Thus, in 2013, the UN Group of Governmental Experts identified some fundamental recommendations on CBMs, which included the need to enhance information sharing among States on ICT security incidents for timely response, recovery and mitigation actions, including through the exchange of information between national CERTs bilaterally.

While expanding the dialogue on ICT security at the international level, paradoxically, we have moved away from these goals, which have been replaced by opportunistic decisions in the interest of particular States. Despite the urgent need to seek strengthened ICT security cooperation, restrictive and discriminatory measures are taken against CERTs. In this regard, it is necessary to address one of the most pressing issues of the international information security agenda: a lack of an adequate level of interaction between the national ICT-security authorities.

Situation

The current situation is characterized by growing distrust, tension and risk of conflict in information space. Nowadays, international community needs a mechanism to assess the disputes in an objective manner and prevent the risks of conflict stemming from the use of ICTs.

From our point of view, the first step towards the creation of such a mechanism includes a global Points of Contact (PoCs) Directory. The establishment of the PoCs

Directory is recommended in the consensus progress report of the Open-ended Working Group (OEWG) on Security of and in the Use of ICTs 2021-2025 as the first universal CBM. At the same time, it is only a result-oriented PoCs Directory that will allow for greater predictability, strengthened trust in information space, as well as setting a foundation for further cooperation. In addition, its development will reaffirm the commitment of the UN Member States to resolve international disputes arising from the use of ICTs by peaceful means.

ICT Security Interaction

Well-established ICT security interaction at the national and international levels contributes to shortening the time of response, reducing the damage caused and strengthening the overall ICT security capacity of States. It is especially important when holding, for example, major international and political events. According to our experience, the potential of such cooperation has not fully unfolded, which may greatly increase the transparency of international information space. The statistics of cooperation of the Russian National Computer Incident Response and Coordination Center (NCIRCC) with the relevant foreign authorities clearly confirm the abovementioned arguments.

In 2019, the NCIRCC sent 2083 notifications on malicious activity directed against the Russian information resources to relevant foreign organizations. As a result, only 550 responses were received.

In 2020, 2897 notifications on malicious activity directed against the Russian information resources were sent, while 649 responses were received.

In 2021, the NCIRCC sent 3303 notifications and received 1697 responses.

The dynamics show that the number of incidents continues to grow year by year, but response measures are taken in half of the cases at best.

Reasons to Ignore Notifications

The reasons for the lack of response to these notifications generally include organizational, legal, technical and political aspects.

For example, international level problems are caused by the lack of unified interaction regulations in the field of computer incident response. Since binding norms

as well as formal agreements do not exist, some States simply ignore the relevant requests.

At the national level, States are prevented from building an effective CERT-to-CERT cooperation by the failure to appoint the single "entry point", i.e. a specific state organization authorized to coordinate actions in the field of detection, prevention and elimination of the consequences of computer attacks, as well as response to computer incidents. As a result, the initiating party lacks detailed understanding of a specific addressee, while the receiving party lacks an adequate authority to process the request and take the relevant measures.

Significant difficulties are caused by the politicization of issues that are technical in origin. Thus, ignoring technical aspects of ICT security creates prerequisites for groundless accusations of targeted State-sponsored computer attacks carried out by the opponents. These aspects include, for instance, lack of reliable and accurate instruments to identify sources of malicious activities, the spreading practice of providing computer attack tools within the framework of a service model (Malware-as-a-Service, Attack-as-a-Service), as well as lack of transparency of the existing Internet protocols. Political attribution can be used to discredit reputation of States, exert pressure or coerce to actions that are not in the national interests. Hence, the involvement of technical experts will facilitate making all the necessary conclusions, identifying those responsible and taking relevant decisions on the basis of a comprehensive data analysis.

Pragmatic PoCs Directory

In this regard, the Russian Federation proposes to establish a pragmatic and depoliticized PoCs Directory that will allow political and technical experts of the UN Member States to provide prompt assistance to each other and overcome tensions that may stem from malicious use of ICTs.

The establishment of the PoCs Directory at the UN will contribute to addressing the following tasks:

- *Designating points to be contacted by competent authorities in their countries or abroad in case of incidents, to facilitate communication and*

dialogue on security of and in the use of ICTs;

- *Keeping updated the directory of main contacts for information exchange on computer incidents which need to be addressed immediately;*
- *Establishing pragmatic cooperation between main national organizations on computer incident response;*
- *Easing and overcoming tensions, as well as the threat of conflict arising from misunderstanding and misperception of incidents in ICT security.*

One positive example of such work concerns all the procedures of cooperation between the PoCs developed by the CSTO Coordinating Center for Computer Emergency Response (CCC CSTO). Within its framework technical experts of Member States take practical steps to organize interaction between authorized bodies, exchange information on computer incidents and relevant threats, provide mutual assistance, conduct joint training, etc.

As a national contribution to the OEWG, the Russian Federation disseminated the concept paper on establishing a global PoCs Directory at the UN. One should note that the working principles of the Directory are to be worked out and agreed up on as accurately as possible due to the non-binding nature of CBMs.

We deem necessary to build the work of the PoCs directory within the UN on the following guiding principles:

- *The PoCs Directory within the UN should foster communication and dialogue on security of and in the use of ICTs;*
- *Regardless of the international situation, the PoCs will aim at preserving political neutrality, maintaining interaction with other PoCs on addressing threats to security of and in the use of ICTs;*
- *The PoCs should not be subject to sanctions;*
- *The PoCs will opt for pragmatic interaction on addressing threats to security of and in the use of ICTs in order to exclude risks of misperception, escalation and conflicts which can arise from the use of ICTs;*
- *In their activities PoCs should take into account the recommendations elaborated by the OEWG and follow the rules, norms and principles of*

responsible behaviour of States in information space.

It is also necessary to make sure that the appointed PoCs have an adequate authority to address relevant tasks at the national level.

The PoCs Directory will comprise national authorities of the UN Member States authorized to address issues in the following areas:

1 *Developing international cooperation, as well as establishing bilateral and multilateral contacts on ensuring information security (diplomatic PoC);*

2 *Detecting, preventing and eliminating consequences of computer attacks, as well as computer incident response (technical PoC).*

The Directory should be focused on practical results in reducing and overcoming tensions as well as the risks of conflict that may stem from misunderstanding and misperception of ICT security incidents.

A look forward

The PoCs Directory alone is not enough to establish an effective conflict prevention mechanism. Since the Directory is a core of the future mechanism that makes it possible to send targeted notifications to peer-organizations, some accompanying measures are necessary to be taken in order to strengthen cooperation. As an additional step, it is proposed to consider the development and adoption of Interaction Procedures on security of and in the use of ICTs that can be used by the national authorities to determine specific steps of political and technical PoCs in order to overcome disputes and resolve inter-State tensions.

It will facilitate well-defined and simplified interaction procedures between the UN Member States' authorities through identifying the main areas and forms of their cooperation. The Interaction Procedures will include a basic scenario for the UN Member States in the event of computer attacks carried out against their information infrastructure and / or computer incidents.

These instruments would create prerequisites for further steps, for example, to develop a standardized template of basic information that is required to study a computer attack and a computer incident. It will unify the exchange of ICT security information in order to enhance the effectiveness of response to the relevant threats.

This kind of practice is successfully implemented within the framework of the CCC CSTO, where the PoCs cooperation is clearly regulated and carried out in accordance with the mutually agreed templates. They include information on malicious activity and do not contain sensitive information on the internal network structure, organized processes, employees, etc.

To conclude, an objective assessment of regional CBMs implementation efforts is needed by the UN Member States to learn from both positive and negative experience of the existing Directories. It is important to move on gradually, strengthening our cooperation step by step. We believe that at the first stage the main efforts should be focused on the composition and working principles of the PoCs Directory, as well as the Interaction Procedures and standardized notification templates.

Template for the UN PoCs Directory

UN Member State				
PoC	**Organization (webpage)**	**E-mail**	**Phone**	**Languages**
Diplomatic				
Technical				

1 An organization of a UN Member State authorized at the national level to develop international cooperation, as well as to establish bilateral and multilateral contacts in the field of information security is appointed as a diplomatic PoC.

2 An organization of a UN Member State authorized at the national level to detect, prevent and eliminate the consequences of computer attacks, as well as to respond to computer incidents, is appointed as a technical PoC.

3 E-mail is indicated based on the possibility of sending notifications of computer attacks and incidents to this address for further interaction, as well as other information for the purposes provided for in the concept paper.

4 A contact phone number is indicated, which may not be tied to a specific person and by which you can contact a diplomatic or technical PoC at any available time.

5 The languages spoken by contact persons for communication are indicated